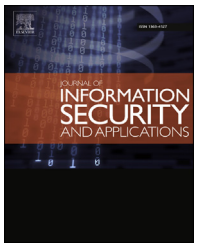
Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa



A secure remote user mutual authentication scheme using smart cards

Marimuthu Karuppiah [a,*], *R. Saravanan* [b]

[a] *School of Computing Science and Engineering, VIT University, Vellore 632014, Tamilnadu, India*
[b] *School of Information Technology and Engineering, VIT University, Vellore 632014, Tamilnadu, India*

ARTICLE INFO

Article history:
Available online 6 November 2014

Keywords:
Remote user authentication
Password
Smart cards
Security
Hash function

ABSTRACT

Authentication thwarts unauthorised users from accessing resources in insecure network environments. Password authentication based on smart cards is one of the simplest and most efficient authentication methods and is commonly deployed to authenticate the legitimacy of remote users. Based on cryptographic techniques, several password authentication schemes have previously been implemented. However, all of these schemes are vulnerable to various malicious attacks that are discussed below. In this paper, we propose a secure remote user mutual authentication scheme using smart cards that achieves all security requirements. Furthermore, we show that our proposed scheme can withstand various malicious attacks and is more suitable for practical applications than other related schemes.

1. Introduction

With recent advancements in Internet and e-commerce technologies, many services, such as online gaming, online shopping, e-learning, e-health, Internet banking, online trading, etc., are offered through the Internet which make life very convenient. However, with increases in various malicious attacks, such as replay attacks, password-guessing attacks, server-spoofing attacks, etc., network and information security has become an important issue for Internet-based services. Authentication is a method for verifying the identities of remote users in Internet environments before they can access a service. Generally, there are three types of authentication methods 1. Identity authentication of something known, such as password. This is called single factor authentication. 2. Identity authentication of something possessed, such as smart cards. This is called two-factor authentication. 3. Identity authentication of some personal characteristics, such as fingerprint, voiceprint and iris scan. This is called three-factor authentication. Most early authentication schemes are only based on password. While such schemes are relatively easy to execute, passwords have several vulnerabilities (Klein, 1990). Smart card based password authentication provides two-factor authentication, that is a successful login requires the user to have a legal smart card and a proper password. Three-factor authentication is very similar to smartcard based password authentication, with the only difference that it requires biometric characteristics as an additional authentication factor (Huang et al., 2011; He et al., 2014). However, there is a risk in using biometric factor that most people do not like to talk about, but it is important to consider. People suffer from accidents all the time. In some serious cases, these lead to disfiguration of hands, eye damage, vocal chord damage, etc. Notwithstanding these, even the implementation cost is too high. As a

* *Corresponding author.*
E-mail addresses: k.marimuthu@vit.ac.in, marimuthume@gmail.com (M. Karuppiah), rsaravanan@vit.ac.in (R. Saravanan).
http://dx.doi.org/10.1016/j.jisa.2014.09.006

result, three-factor authentication is more expensive than single or two-factor authentication. Due to these concerns, the password authentication scheme using smart card is one of the simplest and most convenient authentication methods for handling secret data in insecure network environments. Several password authentication schemes using smart cards have been proposed in the past, some of which are discussed below.

In 1981, Lamport (1981) proposed a password-based remote user authentication scheme that used a one-way hash function. However, Lamport's method has three drawbacks: 1) high hash overhead; 2) the necessity of password resetting; and 3) the requirement that a password table be stored on the server to verify the legitimacy of a user. Since the initial proposal of Lamport's scheme, several improved password-based authentication schemes (Shimizu, 1991; Neil, 1994; Sandirigama and Shimizu, 2000; Chen and Lee, 2008; Hwang, 1983; Harn et al., 1989; Shieh et al., 1997) have been proposed to overcome drawbacks 1 and 2. A common characteristic of all of these schemes is the verification table, which is stored securely on the server and contains the user's password. If an adversary steals or modifies the verification table, the system partially or totally breaks. To overcome this drawback, a non-interactive password authentication without password tables was proposed by Hwang et al. (1990) in 1990; this authentication scheme requires the use of a smart card by the user, the login credentials of the user are not stored by the server. The main drawback in this scheme is that the password cannot be modified easily. Since there is a one-to-one correspondence between the ID_i and the password PWD_i, if the password PWD_i has to be changed into PWD_i' for some security reasons, then the ID_i also has to be changed. However, it is infeasible to change a user's ID. In 1991, Chang and Wu (1991) proposed a remote user password authentication scheme using smart cards. One year later (1992), Chang's and Wu's scheme was broken by Chang and Laih (1992). They assumed that the information stored on the smart card could be easily read out by a smart card user. Using the public information of a smart card, the user derives the secret key. Therefore, he/she can find another user's password by intercepting the login transmitting message. Subsequently, many authors proposed different authentication schemes with smart cards (Chang and Hwang, 1993; Shiuh-Jeng and Jin-Fu, 1996; Yang and Shieh, 1999; Chang and Hwang, 1993; Shiuh-Jeng and Jin-Fu, 1996; Yang and Shieh, 1999).

In 2000, Hwang and Li (2000) proposed a verifier-free password authentication scheme that uses smart cards and is based on ElGamal's public key technique (ElGamal, 1985a). However, Hwang et al.'s scheme does not allow users to freely choose and change their passwords. Furthermore, Hwang et al.'s scheme has been found to be vulnerable to various impersonation attacks (Chan and Cheng, 2000; Chang, 2003; Her-Tyan et al., 2004).

To improve efficiency, Sun (2000) proposed an efficient remote user authentication scheme that uses smart cards and is based on cryptographic hash functions. The major drawbacks of the scheme of Sun et al. are that the passwords are not easily memorisable and that the user cannot freely choose or change his/her password. In 2002, Chien et al. (2002) criticised the scheme of Sun et al. by pointing out that this scheme only achieves one-sided user authentication and subsequently proposed an enhanced verifier-free password authentication scheme that is capable of mutual authentication. Additionally, the user can freely choose his/her password in the scheme of Chan and Cheng (2001) showed that Shieh et al.'s authentication scheme (Yang and Shieh, 1999) was insecure against forgery attack.

In 2003, Sun and Yeh (2003) pointed out LM. Cheng et al.'s attack cannot work in scheme (Yang and Shieh, 1999), since the attacker forged an invalid identity which does not exist in the server's verification table. Therefore, the attacker cannot be verified from verification table. At the same time, Sun and Yeh (2003) showed that Shieh et al.'s scheme was vulnerable to the forgery attack. Later, Shen et al. (2003) improved Shieh et al.'s authentication scheme to withstand LM. Cheng et al.'s attack. However, Yang et al. (2004) pointed out that Shen et al.'s scheme was still vulnerable to the forgery attack.

In 2004, Hsu (2004) offered the criticism that Chien et al.'s scheme (Chien et al., 2002) cannot resist parallel session attacks, and Ku and Chen (2004) also claimed that Chien et al.'s scheme cannot resist reflection attacks and insider attacks. Additionally, Ku and Chen (2004) proposed an improved version of Chien et al.'s scheme with increased security strength against reflection attacks and insider attacks. Unfortunately, Yoon et al. (2004) proved that Ku et al.'s scheme is vulnerable to parallel-session attacks and uncommon denial-of-service attacks, and these authors proposed a slightly modified version of Ku et al.'s scheme. Later, Kumar proved that Yoon et al.'s scheme is still vulnerable to the parallel session attack, and Hsiang and Shih (2009) also claimed that Yoon et al.'s scheme is vulnerable to masquerading attack, offline password guessing attacks and parallel session attack and then proposed an improved scheme to remedy these defects. In 2005, Lee et al. (2005) improved Chien et al.'s scheme by adding the ability to resist parallel session attacks. Subsequently, several authentication schemes (Kim et al., 2005; Lu and Cao, 2005; Fan et al., 2005; Lee and Chiu, 2005) have been proposed.

In 2006, Liao et al. (2006) proposed a password authentication scheme that could be implement over insecure networks. Unfortunately, Yoon and Yoo (2006) and Xiang et al. (2008), respectively, showed that Liao et al.'s scheme is vulnerable to offline password guessing attacks, replay attacks, and denial-of-service attacks. However, none of these authors suggested any remedies for the vulnerabilities to these attacks. Later, Kumar et al. (2011) improved Liao et al.'s scheme by enabling it to resist the attacks pointed out by EJ. Yoon et al. and Xiang et al. In the same year, many remote user authentication schemes (Lin et al., 2006; Shieh and Wang, 2006; Liaw et al., 2006; Peyravian and Jeffries, 2006) were proposed. In 2007, Wang et al. (2007) proved that both Ku and Chen (2004) and Yoon et al. (2004) schemes cannot resist forgery attacks, denial-of-service attacks or offline password guessing attacks. Additionally, these authors proposed an improved scheme for real applications in resource-limited environments.

In 2008, Chung et al. (2009) proved that Wang et al.'s scheme is vulnerable to offline password guessing attacks and impersonation attacks and is unable to achieve perfect forward secrecy (Diffie et al., 1992). Additionally, these authors